#4

S/N To be assigned

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	KILKKILÄ	Serial No.:	To be assigned
Filed:	10/11/01	Docket No.:	602.352USW1
Title:	METHOD AND SYSTEM FOR SELECTING A PASSWORD ENCRYPTED WITH A CORRECT SOFTWARE VERSION		

CERTIFICATE UNDER 37 CFR 1.10
'Express Mail' mailing label number: EL 887040869 US
Date of Deposit: 11 October 2001
I hereby certify that this correspondence is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C . 20231.

By: Kari Arnold
Name: Kari Arnold

SUBMISSION OF PRIORITY DOCUMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is a certified copy of Finnish application, Serial Number 990805, filed 13 April 1999, the priority of which is claimed under 35 U.S.C. §119.

Respectfully submitted,

Altera Law Group, LLC
6500 City West Parkway
Suite 100
Minneapolis, MN 55344-7701
(952)-912-0527

Date: 11 October 2001

By:
Michael B. Lasky
Reg. No. 29,555
MBL/vlb

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 29.8.2001

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	**Nokia Telecommunications Oy** **Helsinki**
Patenttihakemus nro Patent application no	**990805**
Tekemispäivä Filing date	**13.04.1999**
Kansainvälinen luokka International class	**H04M 3/22**

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä tiedon välittämiseksi puhelinkeskus-järjestelmässä"

Hakijan nimi on hakemusdiaariin **12.12.1999** tehdyn nimenmuutoksen jälkeen **Nokia Networks Oy.**

The application has according to an entry made in the register of patent applications on **12.12.1999** with the name changed into **Nokia Networks Oy.**

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

MENETELMÄ JA JÄRJESTELMÄ TIEDON VÄLITTÄMISEKSI PUHELINKESKUSJÄRJESTELMÄSSÄ

KEKSINNÖN ALA

Esillä oleva keksintö liittyy tietoliikennejärjestelmiin. Erityisesti keksinnön kohteena on uuden tyyppinen menetelmä ja järjestelmä oikealla ohjelmistoversiolla salatun salasanan valitsemiseksi puhelinkeskusjärjestelmässä.

TEKNIIKAN TASO

Puhelinverkko koostuu yleensä useista erillisistä puhelinkeskuksista, jotka on kytketty toisiinsa siirtojohdoilla. Puhelinverkkoa hallitaan ja huolletaan käytönohjausverkolla (O&M-network, Operation and Maintenance), joka voidaan toteuttaa esimerkiksi X.25-pakettiverkon palveluihin pohjautuen. Käytönohjausverkko muodostetaan kytkemällä puhelinkeskukset ja muut ohjauksen alaiset verkkokomponentit siihen. Muita ohjauksen alaisia verkkokomponentteja ovat esimerkiksi transkooderi (TC, TransCoder), tukiasema (BTS, Base Transciever Station) ja tukiasemaohjain (BSC, Base Station Controller). Puhelinverkon käyttötoimet keskitetään pääasiassa valvomoihin ja käytönohjauksen keskittäviin verkkoelementteihin. Tällainen keskittävä verkkoelementti voi olla esimerkiksi Nokian valmistama DX 200 OMC.

Keskittävistä puhelinverkkoelementeistä voidaan muodostaa etäistuntoja muihin käytönohjausverkkoon yhdistettyihin puhelinkeskuksiin tai puhelinkeskusjärjestelmiin. Kun etäistunto muodostetaan, lähdejärjestelmä eli esimerkiksi keskittävä verkkoelementti, lähettää käyttäjän tunnistustiedot, käyttäjätunnuksen ja salasanan kohdejärjestelmään. Kohdejärjestelmä on esimerkiksi puhelinkeskusjärjestelmä.

DX 200-puhelinkeskusjärjestelmässä ja käytönohjausverkon käyttöliittymässä (Man Machine Interface, MMI) käyttäjän valtuudet ja oikeudet määräytyvät käyttäjätunnuksen (User ID) perusteella. MMI-järjestelmä on tietty ohjelmiston ja oheislaitteiden muodostama kokonaisuus, jolla voidaan suorittaa käytönohjausfunktioita. Kullekin käyttäjätunnukselle on määritelty yksilöllinen salasana käyttäjän oikeellisuuden todentamiseksi. Tietoturvariskien minimointi edellyttää salasanan vaihtamista riittävän usein, jotta käyttäjätunnuksen käyttöön valtuuttamaton henkilö ei pääse käyttämään käyttäjätunnusta, joka hänelle ei kuuluu.

Edellä mainitussa järjestelmässä on ongelmana se, että salasanan salauksen ohjelmistoversiot voivat olla erilaisia eri verkkoelementeissä. Tällä hetkellä käyttäjän tunnistus etäyhteydellä etenee niin, että käyttäjä syöttää tarvittavan salasanan uudestaan siinä vaiheessa, kun etäistunto aloitetaan, jos ohjelmistoversiot lähdejärjestelmässä ja etäjärjestelmässä poikkeavat toisistaan.

Keksinnön tarkoituksena on poistaa edellä mainitut epäkohdat tai ainakin merkittävästi lieventää niitä.

Erityisesti keksinnön tarkoituksena on tuoda esiin uudentyyppinen menetelmä ja järjestelmä, jonka avulla vältetään salasanan uudelleen syöttö ja parannetaan näin käyttömukavuutta käyttäjän kannalta.

Esillä olevan keksinnön tunnusomaisten seikkojen osalta viitataan patenttivaatimuksiin.

KEKSINNÖN KOHDE

Keksinnön mukainen menetelmä koskee salasanan välitystavan valitsemista tietoliikenneverkossa. Edullisesti keksinnön mukaiseen tietoliikennejärjestelmään kuuluu lähdejärjestelmä, kohdejärjestelmä, käytönohjausverkko, joka on muodostettu lähde- ja kohdejärjes-

telmien välille sekä käytönohjauskeskitin, joka on yhdistetty käytönohjausverkkoon. Lähde- ja kohdejärjestelmät ovat esimerkiksi puhelinkeskusjärjestelmiä. Menetelmässä kirjaudutaan lähdejärjestelmään syöttämällä käyttäjätunnus ja sitä vastaava voimassa oleva salasana. Kun tunnus on syötetty, muodostetaan etäistunto käytönohjauskeskittimen kautta kohdejärjestelmään. Keksinnön mukaisesti tarkistetaan, onko kohdejärjestelmässä käytössä erilainen salasanan salauksen ohjelmistoversio kuin lähdejärjestelmässä. Tarkistuksen voi tehdä sekä lähde- että kohdejärjestelmä.

Lähde- ja/tai kohdejärjestelmään on tallennettu käyttäjätunnusten salasanan salauksen eri ohjelmistoversioihin liittyvät salasanat. Jos kohdejärjestelmän salasanan salauksen ohjelmistoversio on aiempi kuin lähdejärjestelmän, lähetetään kohdejärjestelmälle se salasana, joka liittyy kohdejärjestelmän salasanan salauksen ohjelmistoversioon. Vastaavasti jos kohdejärjestelmän salasanan salauksen ohjelmistoversio on uudempi, lähetetään sille lähdejärjestelmän salasanan salauksen ohjelmistoversioon liittyvä salasana.

Keksinnön mukaiseen järjestelmään kuuluu välineet kohdejärjestelmän ja lähdejärjestelmän salasanan salauksen ohjelmistoversioiden vertaamiseksi keskenään ja välineet aikaisemman ohjelmistoversion mukaisen, kyseessä olevaan käyttäjätunnukseen liittyvän salasanan lähettämiseksi kohdejärjestelmälle.

Eräässä keksinnön mukaisessa sovelluksessa järjestelmään kuuluu välineet lähde- ja/tai kohdejärjestelmän salasanan salauksen eri ohjelmistoversioihin liittyvien käyttäjätunnuksiin kuuluvien salasanojen tallentamiseksi tiettyyn ennalta määrättyyn tilaan.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta käyttäjän ei tarvitse syöttää salasanaa uudestaan ottaessaan etäyhteyttä kohdejärjestelmään. Kohde- ja lähdejärjestelmän salasanan salauksen ohjelmistoversiota

verrataan keskenään ja valitaan tämän perusteella oikea salasana.

KUVALUETTELO

Seuraavassa keksintöä selostetaan yksityiskohtaisesti sovellusesimerkkien avulla, jossa

kuva 1 esittää erästä keksinnön mukaista edullista järjestelmää, ja

kuva 2 esittää erästä keksinnön mukaista etäyhteyden muodostusta vuokaavioesimerkkinä.

KEKSINNÖN YKSITYISKOHTAINEN SELOSTUS

Kuvan 1 mukaiseen järjestelmään kuuluu lähdejärjestelmä LE1, kohdejärjestelmä LE2, käytönohjausverkko OM, joka on muodostettu lähde- ja kohdejärjestelmien (LE1, LE2) välille sekä käytönohjauskeskitin OMC, joka on yhdistetty käytönohjausverkkoon OM. Lähde- ja kohdejärjestelmä ovat edullisesti puhelinkeskusjärjestelmiä. Puhelinkeskusjärjestelmä on esimerkiksi hakijan valmistama DX 200 -puhelinkeskus ja käytönohjauskeskitin OMC on esimerkiksi DX 200 OMC. Lisäksi järjestelmään kuuluu välineet 1 kohdejärjestelmän LE2 salasanan salausversioiden vertaamiseksi keskenään ja välineet 2 aikaisemman ohjelmistoversion mukaisen, kyseessä olevaan käyttäjätunnukseen liittyvän salasanan lähettämiseksi kohdejärjestelmälle LE2. Edelleen järjestelmään kuuluu välineet 3 lähde- ja/tai kohdejärjestelmän (LE1, LE2) salasanan salauksen eri ohjelmistoversioihin liittyvien käyttäjätunnuksiin kuuluvien salasanojen tallentamiseksi tiettyyn ennalta määrättyyn tilaan.

Kuvassa 2 esitetään erästä keksinnön mukaista etäyhteyden muodostusta vuokaavioesimerkkinä. Järjestelmän käyttäjä haluaa muodostaa etäyhteyden valitsemaansa kohdejärjestelmään, lohko 20. Käyttäjä on esimerkiksi operaattori, joka seuraa järjestelmän toimin-

taa. Käyttäjä kirjautuu lähdejärjestelmään syöttämällä käyttäjätunnuksensa ja sitä vastaavan salasanan, lohko 21. Kullekin käyttäjätunnukselle on ennalta määrätty tarkoin rajatut oikeudet. Toisin sanoen käyttäjälle on pääsy ainoastaan niihin toimintoihin, joista on ennalta sovittu.

Muodostetaan edelleen etäistunto käytönohjauskeskittimen kautta haluttuun kohdejärjestelmään, lohko 22. Käyttäjälle läpinäkymättömästi verrataan lähde- ja kohdejärjestelmän salasanan salauksen ohjelmistoversioita keskenään, lohko 23. Seurauksena voi olla kolme erilaista tilannetta, joiden perusteella päätellään kohdejärjestelmään lähetettävä oikea salasana, lohko 24. Kohdejärjestelmän salasanan salauksen ohjelmistoversio on

- sama kuin lähdejärjestelmän, tai
- uudempi kuin lähdejärjestelmän, tai
- aiempi kuin lähdejärjestelmän ohjelmistoversio.

Ensimmäisessä tapauksessa lähetetään kohdejärjestelmälle salasana normaalisti.

Toisessa tapauksessa kohdejärjestelmän täytyy saada ennen salasanojen vertausta tieto siitä, että lähdejärjestelmän ohjelmistoversio on aiempi. Muutoinhan kohdejärjestelmä tulkitsisi salasanan vääräksi ja lopettaisi yhteyden muodostuksen. Kohdejärjestelmässä on tässä tapauksessa tieto käyttäjätunnuksiin liittyvistä salasanojen vaihteluista, jotka liittyvät ohjelmistoversioihin. Näin kohdejärjestelmä osaa verrata vastaanotettua salasanaa oikeaan salasanaan.

Kolmannessa tapauksessa kohdejärjestelmän salasanan salauksen ohjelmistoversio on vanhempi kuin lähdejärjestelmän vastaava. Tässä tapauksessa lähdejärjestelmän täytyy ennen salasanan lähetystä selvittää, mikä ohjelmistoversio kohdejärjestelmällä on. Kun tieto on saatu, lähdejärjestelmä voi lähettää kohdejärjestelmälle oikean salasanan.

Keksintöä ei rajata pelkästään edellä esitettyjä sovellusesimerkkejä koskevaksi, vaan monet muunnokset ovat mahdollisia pysyttäessä patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.

PATENTTIVAATIMUKSET

1. Menetelmä oikealla ohjelmistoversiolla salatun salasanan valitsemiseksi tietoliikennejärjestelmässä, johon kuuluu:

lähdejärjestelmä (LE1);

kohdejärjestelmä (LE2);

käytönohjausverkko (OM), joka on muodostettu lähde- ja kohdejärjestelmien välille; ja

käytönohjauskeskitin (OMC), joka on yhdistetty käytönohjausverkkoon (OM),

joka menetelmä käsittää vaiheet:

kirjaudutaan lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava voimassa oleva salasana,

muodostetaan etäistunto käytönohjauskeskittimen (OMC) kautta kohdejärjestelmään (LE2),

tarkistetaan salasanan oikeellisuus lähde- ja/tai kohdejärjestelmässä (LE1, LE2) vertaamalla salasanaa lähde- ja/tai kohdejärjestelmään (LE1, LE2) tallennettuun käyttäjätunnusta vastaavaan salasanaan,

t u n n e t t u siitä, että menetelmä käsittää vaiheet:

verrataan kohdejärjestelmän (LE2) ja lähdejärjestelmän (LE1) salasanan salauksen ohjelmistoversioita keskenään; ja jos lähde- ja kohdejärjestelmän salasanan salauksen ohjelmistoversiot poikkeavat toisistaan;

lähetetään kohdejärjestelmälle (LE2) kyseessä olevan käyttäjätunnukseen liittyvä salasana, joka on salattu aikaisemmalla salasanan salauksen ohjelmistoversiolla.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että verrataan salasanan salauksen ohjelmistoversioita kohde- ja/tai lähdejärjestelmässä (LE2, LE1).

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että tallennetaan lähde- ja/tai kohdejärjestelmään (LE1, LE2) käyttäjätunnuksen

salasanan salauksen eri ohjelmistoversioihin liittyvät salasanat tiettyyn ennalta määrättyyn tilaan.

4. Järjestelmä oikealla ohjelmistoversiolla salatun salasanan valitsemiseksi tietoliikennejärjestelmässä, johon kuuluu

lähdejärjestelmä (LE1);

kohdejärjestelmä (LE2);

käytönohjausverkko (OM), joka on muodostettu lähde- ja kohdejärjestelmien (LE1, LE2) välille; ja

käytönohjauskeskitin (OMC), joka on yhdistetty käytönohjausverkkoon (OM), jossa järjestelmässä:

kirjaudutaan lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava voimassa oleva salasana,

muodostetaan etäistunto käytönohjauskeskittimen (OMC) kautta kohdejärjestelmään (LE2),

tarkistetaan salasanan oikeellisuus lähde- ja/tai kohdejärjestelmässä (LE1, LE2) vertaamalla salasanaa lähde- ja/tai kohdejärjestelmään (LE1, LE2) tallennettuun käyttäjätunnusta vastaavaan salasanaan,

t u n n e t t u siitä, että järjestelmään kuuluu:

välineet (1) kohdejärjestelmän (LE2) salasanan salausversioiden vertaamiseksi keskenään; ja

välineet (2) kohdejärjestelmän (LE2) ohjelmistoversion mukaisen, kyseessä olevaan käyttäjätunnukseen liittyvän salasanan lähettämiseksi kohdejärjestelmälle (LE2).

5. Patenttivaatimuksen 4 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmään kuuluu välineet (3) lähde- ja/tai kohdejärjestelmän (LE1, LE2) salasanan salauksen eri ohjelmistoversioihin liittyvien käyttäjätunnuksiin kuuluvien salasanojen tallentamiseksi tiettyyn ennalta määrättyyn tilaan.

6. Patenttivaatimuksen 4 tai 5 mukainen järjestelmä, t u n n e t t u siitä, että lähde- ja/tai kohdejärjestelmä (LE1, LE2) on puhelinkeskusjärjestelmä.

(57) **TIIVISTELMÄ**

Menetelmä ja järjestelmä oikealla ohjelmistoversiolla salatun salasanan valitsemiseksi tietoliikennejärjestelmässä. Keksinnön mukaiseen järjestelmään kuuluu lähdejärjestelmä (LE1), kohdejärjestelmä (LE2), käytönohjausverkko (OM), joka on muodostettu lähde- ja kohdejärjestelmien (LE1, LE2) välille sekä käytönohjauskeskitin (OMC), joka on yhdistetty käytönohjausverkkoon (OM). Menetelmässä kirjaudutaan lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava salasana. Edelleen muodostetaan etäistunto käytönohjauskeskittimen (OMC) kautta kohdejärjestelmään (LE2). Keksinnön mukaisesti verrataan kohdejärjestelmän (LE2) ja lähdejärjestelmän (LE1) salasanan salauksen ohjelmistoversioita keskenään; ja jos lähde- ja kohdejärjestelmän salasanan salauksen ohjelmistoversiot poikkeavat toisistaan; lähetetään kohdejärjestelmälle (LE2) kyseessä olevan käyttäjätunnuksen se salasana, joka liittyy aikaisempaan salasanan salauksen ohjelmistoversioon.

(Fig. 1)

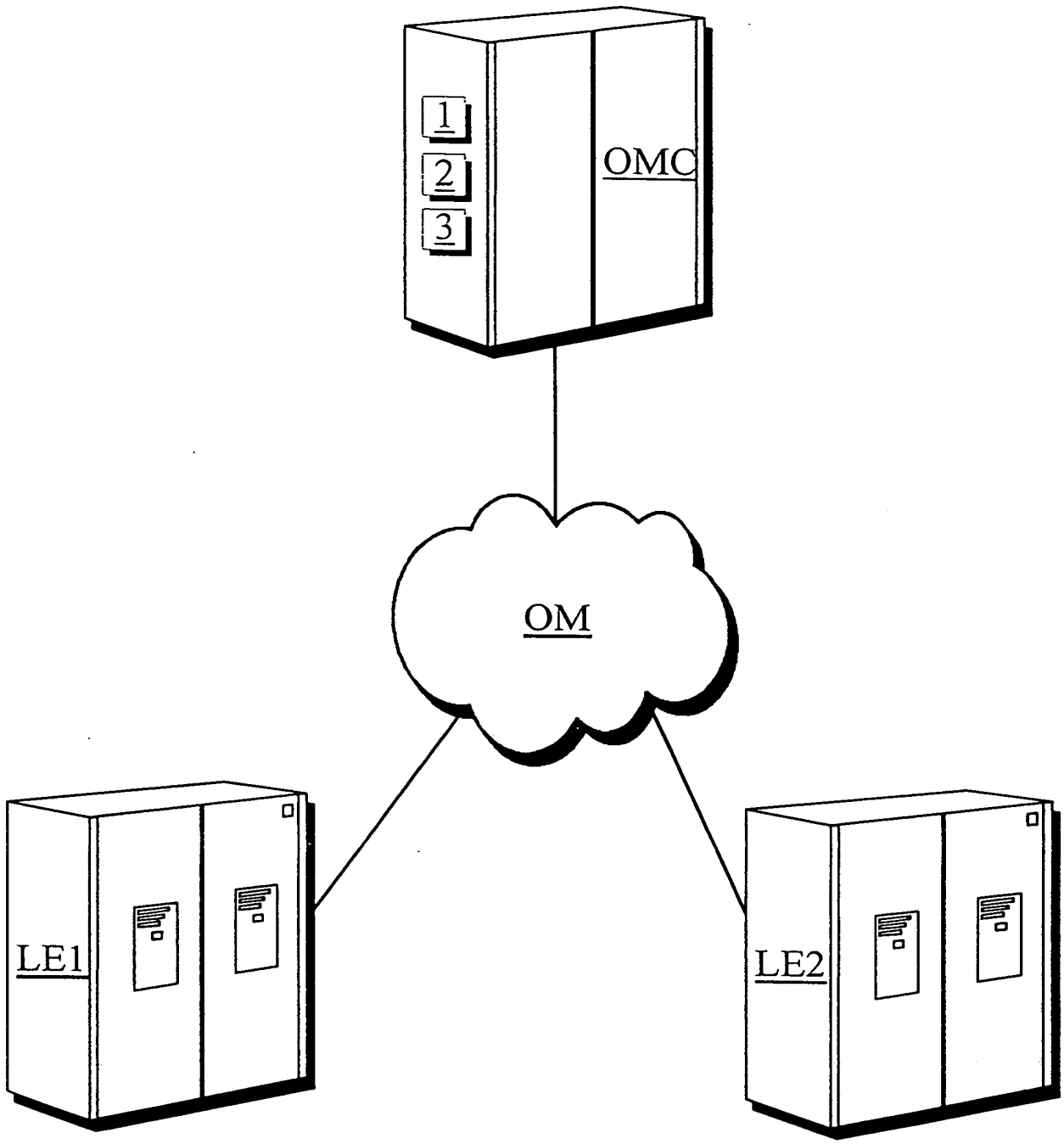

Fig.1

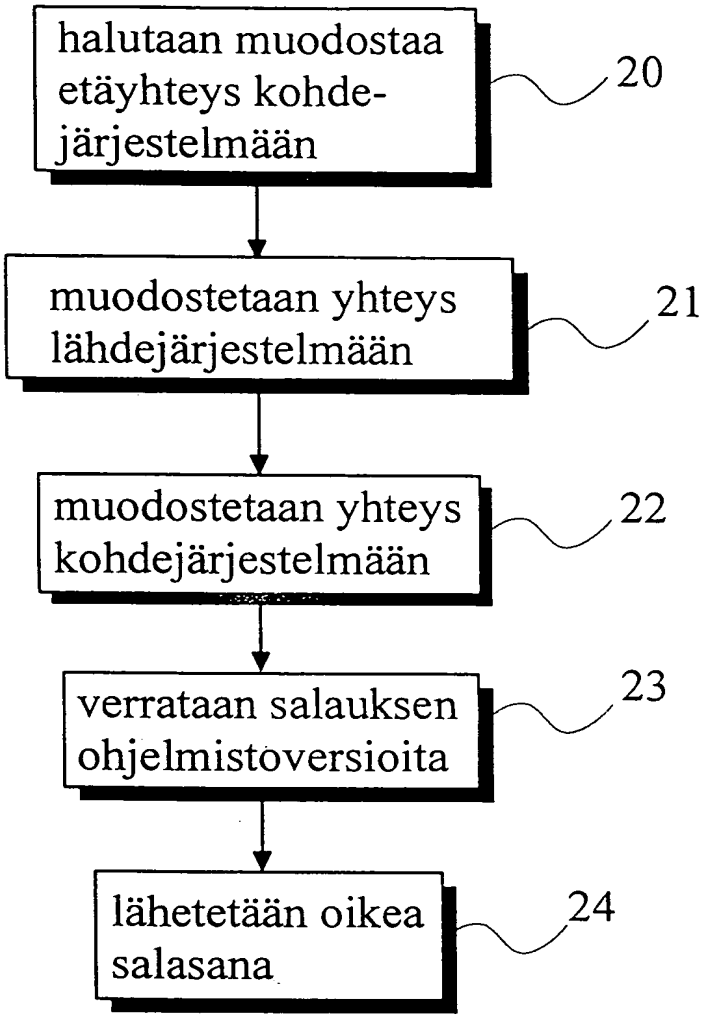
halutaan muodostaa etäyhteys kohde-järjestelmään
20
muodostetaan yhteys lähdejärjestelmään
21
muodostetaan yhteys kohdejärjestelmään
22
verrataan salauksen ohjelmistoversioita
23
lähetetään oikea salasana
24

Fig.2